I claim:

1. A method of promoting the purchase of a fully functional product delivered in digital form comprising the steps of:

creating a fully functional version of said product with a defined limited functionality;

assigning a unique product identifier to said product;

delivering to at least some new users said fully functional product configured to operate in a limited functionality mode; and

arranging said product such that at least some of said new users are offered the option of procuring an authorization for a fully functioning product; wherein said authorization procurement includes the steps of:

(a) generating an operating context identifier associated with at least one measurable factor of the operating context of said user;

(b) transmitting a request comprising the unique product identifier and the operating context identifier to a licensing system acting on behalf of one or more licensors;

(c) receiving an encoded message from said licensing system to authorize the product to operate in the fully functional mode for the operating context; and

(d) permitting the product to operate in the fully functional mode as long as said at least one measurable factor remains within acceptable limits;

whereby said product returns to said limited functionality mode when a user attempts to operate the product in a different operating context.

2. The method of claim 1 in which said operating context depends on at least one reliably measurable characteristic of the user or the user's system.

3. The method of claim 2 in which said at least one reliably measurable characteristic is selected from the set of: machine-readable user-identifier, serial number of user processor or product, distinguishing features of the user's processor, user's voice pattern, spoken or typed password, processor time-stamp, nearly unique tattoo, telephone number, network address, user's visual appearance, and biological tissue samples.

4. The method of claim 1 in which said unique product identifier is associated with at least one predefined licensor of said product.

5. The method of claim 1 in which said licensing system uses said product identifier to credit a corresponding licensor according to the number of authorizations for said product identifier.

6. The method of claim 1 in which said licensing system uses said operating context identifier to modify information in a corresponding user account record.

7. The method of claim 1 in which said licensing system uses said operating context identifier to debit an account associated with said operating context identifier, and said licensing system uses said product identifier to credit a corresponding licensor's account according to the number of authorizations for said product identifier.

8. A method for limiting access to selected features of a multimedia file, comprising the steps of:

disabling selected features of said multimedia file;

distributing said multimedia file with at least some enabled features;

offering to enable one or more specific disabled features when a user attempts to use at least one of said specific disabled features;

receiving a request from a user or user's system, said request identifying an operating context and identifying said one or more disabled features; and

transmitting an authorization to said user or user's system to enable said one or more disabled features, where said authorization is uniquely associated with said operating context ;

whereby said selected features remain enabled only for said operating context.

9. The method of claim 8 further comprising the step of:

identifying an operating context and a licensor from information in said request and arranging to send an authorization according to an agreement between said user and said licensor.

10. The method of claim 8 further comprising the steps of:

providing a user environment in which pre-defined actions by said user are interpreted as a request for access to at least some of said disabled features;

creating an identifier for said operating context, wherein said identifier is created according to at least one measurable factor of said user's user environment; and

using said operating context identifier to associate said authorization with said user's operating context;

whereby said authorization will not enable said disabled features when said at least one measurable factor has changed beyond a pre-configured limit.

11. The method of claim 8 in which said at least one measurable factor is selected from the set of:

machine-readable user identifier serial number of user processor or product, machine-readable features of the user's system, user's voice pattern, spoken or typed password, processor time-stamp, nearly unique tattoo, telephone number, network address, user's visual appearance, and biological tissue samples

12. The method of claim 8 further comprising the steps of:

ensuring that an authorization received for one or more selected features for said unique user cannot be used for access by another user or on another system; and

permitting use of said at least some enabled features in a different operating context ;

whereby users can obtain authorization to test or demonstrate said selected features on one system and provide additional copies of the multimedia file to others who must then request their own authorizations.

13. A method for limiting access to selected features of a data object, comprising the steps of:

compressing or encrypting portions of said data object;

distributing said data object with at least some operable features;

offering to decompress or decrypt one or more portions of said data object when a user of one of said operable features attempts to use features of at least one of said compressed or encrypted portions;

receiving a request from a user or user's system, said request identifying an operating context and said one or more compressed or encrypted portions;

transmitting an authorization to said user or user's system to decompress or decrypt at least one compressed or encrypted portion, where said authorization is uniquely associated with said unique user;

whereby said selected portion is decompressed or decrypted only for said identified operating context.

14. The method of claim 13 further comprising the steps of:

providing a user environment in which pre-defined actions by said user are interpreted as a request for access to at least some of said compressed or encrypted features;

creating a unique identifier for identifying said operating context according to at least one measurable factor of said user's user environment; and

using said unique identifier to associate said authorization with said user's user environment;

whereby said authorization will not enable decompression or decryption of said compressed or encrypted portion when said at least one measurable factor has changed beyond a pre-configured limit.

15. A method for limiting access to selected data features of copyable encoded information accessed by a user on a user's system, and for restricting access to said selected data features to a particular operating context, comprising the steps of:

locking said selected data feature, having a feature identifier , with a corresponding key;

receiving an unlock request, from the user or user's system, said request having a operating context identifier and a feature identifier;

transforming said key using at least said unique operating context identifier to form an authorization ;

transmitting said authorization to said user or user's system;

reverse transforming said authorization using said unique operating context identifier to obtain the key corresponding to said feature identifier; and

using said key to temporarily unlock said selected data feature;

whereby said authorization can only be used to access the selected data feature in the presence of said operating context identifier.

16. The method of claim 15 in which said operating context identifier is generated according to a pre-determined combination of values selected from the set of: measurable parameters of a user's system, measurable physical information about the user, and information supplied by the user.

17. The method of claim 15 in which said operating context identifier is generated for each unlock request according to the present state of a pre-determined combination of values collected by a user's system.

18. The method of claim 15 in which said feature identifier is generated using unique identification information about said selected data feature in combination with said operating context identifier.

19. The method of claim 15 in which said transforming step uses encryption.

20. The method of claim 15 further comprising the steps of:

retrieving an authorization that has been previously stored for said selected data feature;

reverse transforming said retrieved authorization to obtain a valid key; and

unlocking said feature with said valid key;

whereby a selected data feature once unlocked remains unlockable in the presence of said previously stored authorization and said operating context under pre-determined conditions.

21. The method of claim 15 further comprising the steps of:

storing at least some of said authorizations received by said user or user's system;

selecting a candidate authorization previously stored for said selected data feature;

validating said selected candidate authorization with a reverse transform using said unique operating context identifier; and

either unlocking said selected data feature, if said selected candidate authorization is successfully validated, or else signaling the user or user's system to obtain a valid authorization.

22. The method of claim 15 wherein:

said transforming step is based upon a prime factorization of an N-digit number using said operating context identifier as a randomization key, where N is chosen to be within the factorization capabilities of a licensing computer but beyond the capabilities of the user or the user 's system, and

said reverse transforming step comprises generating the N-digit number in said user's system, and confirming that said N-digit number is the product of the factorization contained in said authorization.

23. The method of claim 15 in which

said transforming step is based upon use of the operating context identifier as the seed for a complex pseudo-random number generator, and said reverse transforming step confirms that the authorization generated in the user's system corresponds to the authorization received, based upon a transform of the operating context identifier and feature identifier.

24. The method of claim 15 further comprising the step of:

storing at least some of said authorizations received by said user or user's system;

determining whether a valid authorization is stored corresponding to a selected data feature desired by said user using said operating context identifier; and

advertising information to said user regarding purchase of a new authorization for said selected data feature when said user's system determines that a corresponding authorization has not been stored or cannot be validated in the present operating context.

25. The method of claim 24 in which said advertising information includes information selected from the set of: description of the selected data feature, advantages of the selected data feature, cost or other requirements for access to the selected data feature, source identification for obtaining an authorization, identification of an owner or licensor of rights in the selected data feature, and method of obtaining a valid authorization for access to said selected data feature.

26. The method of claim 15 further comprising the steps of:

permitting a user or user's system to operate or access at least some unprotected features of said encoded information;

assisting said user in selection of a selected data feature by disclosing information to said user regarding data features for which no valid authorization is present; and

connecting said user's system to a licensing processor for transmission of said unlock request and for reception of said authorization.

27. The method of claim 15 further comprising the steps of:

said user indicating a desire for a selected data feature beyond any features already operable or already unlocked;

informing the user that the feature is locked, where said feature is locked unless a valid authorization has been stored for said user-ID and said authorization is still valid;

offering said user information about possible benefits of obtaining access to said locked feature;

offering to said user to provide said user with access to said feature upon agreement with predetermined conditions; and

forming an unlock request for a user who indicates agreement with said at least some of said predetermined conditions.

28. The method of claim 15 in which said selected data feature is selected from the following abilities: to decompress encoded information, to access a text file, to execute a software or hardware program, to access a further distribution channel, to decrypt digital data, to enable a high-quality output, to enable storage of processing results, to access a digitized multimedia file, to enable predetermined hardware or software features of the user's system, and to access an analog playback process for an audio, video or multimedia recording.

29. The method of claim 15 in which said selected data features are locked by a transform of either encryption or compression, or both, for which a key is required to reverse each transform; and

a password or authorization provides access to said key;

wherein access to each selected data feature requires a password or authorization which is adequately unique to prevent different users or user's systems from sharing passwords.

30. The method of claim 15 in which at least some of said steps of locking, unlocking, transforming and reverse transforming are carried out in firmware in the user's system.

31. A method for sharing limited access to selected data features of copyable encoded information stored on a server, and for permitting only uniquely identified workstations to unlock said selected data features, comprising the steps of:

locking said selected data feature, having a feature-identifier, with a corresponding key;

receiving an unlock request having a unique workstation-identifier and a feature identifier from the workstation;

transforming said key using at least said unique workstation identifier to form an authorization;

transmitting said authorization to said workstation;

reverse transforming said authorization using said unique workstation identifier to obtain the key corresponding to said feature-identifier; and

using said key to unlock said selected data feature;

whereby said key can only be used to access the selected data feature from a unique workstation-identifier.

32. The method of claim 31 in which authorizations formed for a given workstation are then stored on the server in workstation-specific locations.

33. The method of claim 31 in which said unique workstation identifiers are constructed such that any workstation identified as being on the same network can use the same authorization for the selected data feature of the encoded information.

34. A method of encouraging the purchase of passwords for access to advanced features of encoded information comprising the steps of:

permitting a user or user's system to operate or access at least some unprotected features of said encoded information;

generating a passwordable ID for each advanced feature desired by a user;

generating a target-ID in response to reliably measurable characteristics of the user or user's system;

enabling said user to purchase a password to unlock an advanced feature by forwarding the passwordable ID and other information to a licensing processor;

receiving in said licensing processor said passwordable ID and other information transmitted from the user's system;

providing the user or user's system with the password required for each of the passwordable IDs received;

installing passwords in storage locations accessible to the user or user's system; and

unlocking any advanced features whose passwords have been installed.

35. The method of claim 34 wherein said passwordable ID is made adequately unique by synthesizing the three component IDs: a target-ID specific to the user or user's system, a software-ID, and the feature-ID.

36. The method according to claim 34 wherein said synthesis is achieved by using a uniqueness-preserving combination of at least one of the said three component IDs, using said combination as the seed for a pseudo-random character generation algorithm, and using the first n characters so-generated as the n-digit passwordable ID.

37. The method according to claim 36 wherein said passwordable ID includes an encryption of at least one of said three component IDs.

38. The method according to claim 37 wherein said passwordable ID additionally encrypts other useful information about a user, or about any parties who are to receive payment for the provision of the password.

39. The method of claim 34 further comprising the step of enabling a user to make an informed decision whether to unlock any locked advanced features;

whereby a user is provided with information about the costs and benefits of access to advanced features.

40. The method of claim 34 further comprising the step of arranging for transfer of funds from said user to a software licensor according to said user's target-ID .

41. A method of generating, and encouraging the purchase of authorizations to use licensed features of encoded information, said licensed features including advanced features which are desired by a licensor to be accessible in an operating context only in the presence of an authorization which unlocks said licensed features only in that operating context, said method comprising the steps of:

generating an operating context identifier in response to reliably measurable characteristics of the operating context;

determining whether valid authorizations are present for any licensed features,

unlocking licensed features whose authorizations are present,

enabling a user to make an informed decision whether to unlock any locked licensed features, and

enabling said user to purchase a authorization to unlock a licensed feature by transmitting the corresponding encrypted ID and other information to a licensing processor.

42. The method of claim 41 in which said which said licensed feature is selected from the following abilities: to decompress encoded information, to access a text file, to execute a software or hardware program, to access a further distribution channel, to decrypt encoded digital information, to enable a high-quality output, to enable storage of processing results, to access or decode a digitized multimedia file, to enable predetermined hardware or software features of the user's access device, and to access an analog playback process for an audio, video or multimedia recording.

43. The method of claim 41 further comprising the steps of:

receiving said encrypted identifier and other information transmitted from the user's system;

providing the user or user's system with the authorization required for the encrypted identifier just submitted; and

unlocking any licensed features whose authorizations have been received by the user's system;

wherein the authorization for a given encrypted ID is a predetermined function of the encrypted ID and the validity of a candidate authorization is determined in the user's system.

44. The method of claim 41 which further comprises arranging for transfer of funds from the user to a licensor when enabling said user to purchase an authorization.

45. The method of claim 41 further comprising the steps of:

encrypting predetermined portions of the set of operating context identifiers which are related to the uniqueness of the operating context to create and store a first profile;

comparing said first profile to a new profile generated when a licensed feature has no valid authorization present; and

providing an encrypted difference factor of said comparison to a licensing processor to verify that a user correctly describes changes to the operating context identifiers;

whereby permitted changes to the operating context can be evaluated for issuance of a replacement authorization for said licensed features without requiring additional licensing transactions by said user.

46. The method of claim 41 in which the presence of a valid authorization is determined by comparing the candidate authorization with a result generated by a random character generator using an encrypted operating context identifier as the seed.

47. The method of claim 41 in which the user's system does not contain the full algorithm for generating the authorization for a given licensed feature, and wherein the user's system contains the means of confirming the validity of a stored or received authorization given an identification of a licensed feature.

48. The method according to claim 47 wherein the password is a seed, discovered via algorithms known only to the licensor, which can be used, in conjunction with a random number generator incorporated into the user's system, to generate the encrypted identifier and wherein the presence of a valid authorization is confirmed when the user's system confirms that the candidate authorization can be used as a seed to successfully generate the encrypted identifier.